

CLAIMS

```

1  1.  A method for verification, comprising:
2      providing an implementation model, which defines
3  model states of a target system and model transitions
4  between the model states;
5      providing a specification of the target system,
6  comprising properties that the system is expected to
7  obey;
8      creating a tableau from the specification, the
9  tableau defining tableau states with tableau transitions
10 between the tableau states in accordance with the
11 properties; and
12      comparing the tableau transitions to the model
13 transitions to determine whether a discrepancy exists
14 therebetween.

```

1 2. A method according to claim 1, wherein creating the
2 tableau comprises defining a finite state machine using a
3 hardware description language.

1 3. A method according to claim 2, wherein the
2 implementation model has model inputs and outputs, and
3 wherein defining the finite state machine comprises
4 describing a virtual device having inputs and outputs
5 corresponding to the model inputs and outputs of the
6 implementation model.

1 4. A method according to claim 3, wherein comparing the
2 transitions comprises performing a reachability analysis
3 using both the implementation model and the tableau while
4 providing identical inputs to the inputs of both the
5 implementation model and the tableau, and verifying that
6 the outputs are always identical.

1 5. A method according to claim 4, wherein performing
2 the reachability analysis comprises comparing the model
3 and the tableau automatically using a model checker.

1 6. A method according to claim 4, wherein performing
2 the reachability analysis comprises providing evidence of
3 a tableau transition that is not implemented in the
4 model.

1 7. A method according to claim 1, wherein comparing the
2 tableau transitions comprises associating model
3 transitions with corresponding tableau transitions.

1 8. A method according to claim 7, wherein associating
2 the transitions comprises defining a reachable simulation
3 preorder relating the model and the tableau.

1 9. A method according to claim 7, wherein associating
2 the transitions comprises finding a tableau transition
3 that is not implemented in the model.

1 10. A method according to claim 9, wherein finding the
2 tableau transition that is not implemented in the model
3 comprises deriving an indication, based on the
4 unimplemented transition, that the specification is not
5 complete with respect to the model.

1 11. A method according to claim 9, wherein finding the
2 tableau transition that is not implemented in the model
3 comprises deriving an indication, based on the
4 unimplemented transition, that a transition of the target
5 system is missing in the model.

1 12. A method according to claim 1, and comprising
2 associating model states with corresponding tableau
3 states.

1 13. A method according to claim 12, wherein associating
2 the model states with the corresponding tableau states
3 comprises finding a tableau state that is not implemented
4 in the model.

1 14. A method according to claim 13, wherein finding the
2 tableau state that is not implemented in the model
3 comprises deriving an indication, based on the
4 unimplemented state, that the specification is not
5 complete with respect to the model.

1 15. A method according to claim 13, wherein finding the
2 tableau state that is not implemented in the model
3 comprises deriving an indication, based on the
4 unimplemented state, that a state of the target system is
5 missing in the model.

1 16. A method according to claim 12, wherein associating
2 the model states with the corresponding tableau states
3 comprises finding multiple model states corresponding to
4 a single tableau state.

1 17. A method according to claim 1, wherein creating the
2 tableau comprises creating a reduced tableau from which
3 one or more redundant states have been eliminated.

1 18. A method according to claim 1, wherein comparing the
2 transitions comprises verifying that the specification is
3 a complete and correct description of the implementation
4 model responsive to the comparison.

1 19. A verification processor, which is configured to
2 receive an implementation model, defining model states of
3 a target system and model transitions between the model
4 states, and to receive a specification of the target

5 system, including properties that the system is expected
6 to obey, and which is operative to create a tableau from
7 the specification, the tableau defining tableau states
8 with tableau transitions between the tableau states in
9 accordance with the properties, and to compare the
10 tableau transitions to the model transitions to determine
11 whether a discrepancy exists therebetween.

1 20. A processor according to claim 19, which is
2 operative to perform model checking of the implementation
3 model.

1 21. A computer software product for verification of a
2 specification of a target system, which specification
3 includes properties that the system is expected to obey,
4 by comparison with an implementation model, which defines
5 model states of the target system and model transitions
6 between the model states, the product comprising a
7 computer-readable medium having computer program
8 instructions recorded therein, which instructions, when
9 read by a computer, cause the computer to create a
10 tableau from the specification, the tableau defining
11 tableau states with tableau transitions between the
12 tableau states in accordance with the properties, and to
13 compare the tableau transitions to the model transitions
14 to determine whether a discrepancy exists therebetween.

1 22. A product according to claim 21, wherein the program
2 instructions cause the computer to compare the tableau
3 with the model by running a reachability analysis using
4 both the implementation model and the tableau while
5 providing identical inputs to the inputs of both the
6 implementation model and the tableau, and verifying that
7 the outputs are always identical.

1 24. A product according to claim 21, wherein the
2 instructions cause the computer to verify that the
3 specification is a complete description of the
4 implementation model.

```

2         providing an implementation model, which defines
3 model states of a target system and model transitions
4 between the model states;

```

```

8      creating a tableau from the specification, the
9      tableau defining tableau states with tableau transitions
10     between the tableau states in accordance with the
11     properties; and

```

1 26. A method according to claim 25, wherein creating the
2 tableau comprises defining a finite state machine using a
3 hardware description language.

1 27. A method according to claim 26, wherein the input
2 model has model inputs and outputs, and wherein defining
3 the finite state machine comprises describing a virtual
4 device having inputs and outputs corresponding to the
5 model inputs and outputs of the implementation model.

1 28. A method according to claim 27, wherein comparing
2 the model and the tableau comprises running the model
3 checker while providing identical inputs to the inputs of
4 both the implementation model and the tableau, and
5 verifying that the outputs are always identical.

1 29. A method according to claim 25, wherein comparing
2 the model and the tableau comprises providing evidence of
3 a transition or state in the tableau that is not
4 implemented in the model.

1 30. A method according to claim 29, wherein providing
2 the evidence comprises providing a counter-example
3 indicative of the unimplemented transition or state.

1 31. Model checking apparatus, which is configured to
2 receive an implementation model, defining model states of
3 a target system and model transitions between the model
4 states, and to receive a specification of the target
5 system, including properties that the system is expected
6 to obey, and which is operative to create a tableau from
7 the specification, the tableau defining tableau states
8 with tableau transitions between the tableau states in
9 accordance with the properties, and to compare the
10 tableau to the model by inputting the model and the
11 tableau to an automatic model checking program.

1 32. A computer software product for verification of a
2 specification of a target system, which specification
3 includes properties that the system is expected to obey,
4 by comparison with an implementation model, which defines
5 model states of the target system and model transitions
6 between the model states, the product comprising a
7 computer-readable medium having computer program

35519S3

8 instructions recorded therein, which instructions, when
9 read by a computer, cause the computer to create a
10 tableau from the specification, the tableau defining
11 tableau states with tableau transitions between the
12 tableau states in accordance with the properties, and to
13 compare the tableau to the model by inputting the model
14 and the tableau to an automatic model checking program.

002290"4EE50960